

*cont*

associating the stored selected expiry data with the new digital signature key pair to affect a transition from an old digital signature key pair to a new digital signature key pair.

14. (Thrice Amended) A system for providing updated digital signature key pairs in a public key system comprising:

multi-client manager means for providing selectable digital signature expiry data including at least both public verification key expiry data and [selectable] private signing key expiry data that [is] are selectable on a per client basis wherein the digital signature key pairs are not shared among users;

means, accessible by the multi-client manager means, for digitally storing both selected public key expiry data and selected private key expiry data for association with a new digital signature key pair; and

means, responsive to the stored selected public key expiry data, for associating the stored selected expiry data with the new digital signature key pair to affect a transition from an old digital signature key pair to a new digital signature key pair.

21. (Thrice Amended) A storage medium comprising:

a stored program for execution by a processor wherein the program facilitates providing updated digital signature key pairs in a public key system by:

allowing entry of selectable expiry data including both at least public verification key expiry data and [selectable] signing private key expiry data that are selectable on a per client basis wherein the digital signature key pairs are not shared among users;

digitally storing both selected public key expiry data and selected private key expiry data for association with a new digital signature key pair; and

associating the stored selected expiry data with the new digital signature key pair to affect a transition from an old digital signature key pair to a new digital signature key pair.